CONSENT OF THE NETWORKED

The Worldwide Struggle for Internet Freedom

REBECCA MACKINNON

LIBRARY OF THE
CEU CENTRAL EUROPEAN
UNIVERSITY
BUDAPEST

BASIC BOOKS
A Member of the Perseus Books Group
New York

their broadband provider, mobile phone service, web-hosting service, social networking service, or personal e-mail provider, company policies and practices in dealing with government surveillance are rarely considered. Part of the reason is that it is very difficult for an ordinary person to know what each company is doing and to compare company practices in a meaningful way.

Soghoian suggests that it is possible to "stimulate a market for effective corporate resistance to government access" by mandating greater transparency on the part of corporations and government. If Congress proves incapable of passing laws to require such disclosure, concerned citizens should press state legislatures to pass such disclosure laws, especially in such key states as California, where many Internet companies are located. The result would be greater protection for all customers of companies based in those states, regardless of the jurisdiction in which customers live.

Even if no legislature passes such disclosure laws, however, greater media scrutiny, customer awareness, and user activism might help to push companies in a more citizen-centric direction. But without clear transparency and accountability about how, when, and under what specific circumstances personal information is being collected and used, citizens have good reason to worry about the growth of the state's "panoptic" power.

WIKILEAKS AND THE FATE OF CONTROVERSIAL SPEECH

WikiLeaks and several news organizations that the whistle-blowing organization had chosen as partners published the first batch of classified US diplomatic cables, leaked by disgruntled US Army Private Bradley Manning, in November 2010. Vice President Joseph Biden declared WikiLeaks' leader, Julian Assange, to be a "digital terrorist." Senator Joe Lieberman declared that "WikiLeaks' illegal, outrageous, and reckless acts have compromised our national security and put lives at risk around the world." Meanwhile, the WikiLeaks "Cablegate" website, dedicated

to showcasing the leaked diplomatic cables, came under distributed denial of service attacks of unknown origin. The site was unable to stay online. Assange decided to move the storage and publication of his website's data to another web-hosting service, run by Amazon, which is known for its robustness in defending against cyber-attacks and thus often used by small human rights groups that lack sufficient in-house technical expertise to defend themselves.

Two days after Assange moved the Cablegate site to Amazon, Amazon headquarters received a call of complaint from Lieberman's office. Shortly thereafter, Amazon booted WikiLeaks. The senator responded with a statement: "I wish that Amazon had taken this action earlier based on WikiLeaks' previous publication of classified material. The company's decision to cut off WikiLeaks now is the right decision and should set the standard for other companies WikiLeaks is using to distribute its illegally seized material."

Amazon later insisted that it had acted independently of Lieberman's phone call. At any rate, legally Amazon was off the hook. Controversial speech hosted on Amazon's web servers is not protected in the same way that speech is constitutionally protected in public spaces. The law gives Amazon the right to set its own rules. Amazon's terms of service clearly state that Amazon "reserves the right to refuse service, terminate accounts, remove or edit content in its sole discretion." By clicking "agree," the customer legally consents to "represent and warrant that you own or otherwise control all of the rights to the content" and confirms that the content "will not cause injury to any person or entity."

Despite the absence of criminal charges against—let alone conviction of—anybody involved with publishing the cables, several other companies including PayPal, MasterCard, and EveryDNS proceeded to sever commercial ties with WikiLeaks. Though these companies were within their legal contractual rights to drop any customer for any reason, in dropping WikiLeaks they nonetheless sent a clear signal to their customers: politically controversial speech—even if there is a strong case to be made that it is constitutionally protected—will not always be welcome with us.

It is also important to recognize that some companies tried to resist efforts to silence people who had damaged the US government and its diplomatic effectiveness but who had yet to be formally charged with, let alone convicted of, a crime. In January 2011, the news broke that US government prosecutors had obtained a subpoena requiring Twitter to hand over account information for five people who had been involved with WikiLeaks' publication of classified US diplomatic cables. The subpoena concerned not tweets—which are public to begin with—but private direct messages between users, records of IP addresses (which can help investigators determine the location of the computers or devices from which certain postings were made), and so forth. The government had not established a criminal case against any of these individuals. Twitter's lawyers fought in court for the order to be unsealed, and thus able to be shared without breaking the law. They won, and immediately informed the five individuals of the request made for their information. Asked by the *New York Times* about the case, Twitter spokeswoman Jodi Olson replied, "To help users protect their rights, it's our policy to notify users about law enforcement and governmental requests for their information, unless we are prevented by law from doing so." Several WikiLeaks team members say they suspect that Google and Facebook were served with similar subpoenas. As of August 2011, the two companies had no comment.

The implications of WikiLeaks—and the issues it raises—are extraordinarily complicated, and to be properly understood, they need to be unraveled, with each strand of intention and consequence analyzed separately. Certainly innocent diplomatic sources—including democracy and human rights activists—were harmed or put at risk by the cables' release, and exposing highly sensitive work by capable diplomats may have had a negative effect on relations with governments where the United States has legitimate, even vital foreign policy and national security interests at stake. Yet at the same time, citizens in a number of countries have used some leaked documents to expose government behavior that is clearly unacceptable by any common standards of accountability and responsibility. Regardless of

whether one views the intentions and consequences of WikiLeaks' release of diplomatic cables favorably, the US government's response to WikiLeaks highlights a troubling murkiness, opacity, and lack of public accountability in the power relationships between government and Internet-related companies.

In a speech in February 2011, Secretary of State Hillary Clinton sought to distance the State Department—and the US government more generally—from individual politicians and media commentators who called for Julian Assange's head without any apparent interest in due process. She also made the point that the US government did not pressure private companies such as Amazon and PayPal to sever their ties with WikiLeaks. But through subsequent reporting in newspapers and research by civil liberties lawyers, it has also become clear that the companies were influenced by government statements and opinions. These included a letter by State Department legal adviser Harold Koh, in which he wrote that the "violation of the law is ongoing" as long as WikiLeaks continues to publish the leaked diplomatic cables.

As Harvard legal scholar Yochai Benkler pointed out in a group e-mail discussion with colleagues about WikiLeaks and the State Department's actions (which I am quoting with his permission), Koh's assertion was patently "false, as a matter of constitutional law." The Justice Department has not managed to bring a viable case to a court of law against WikiLeaks or any other entity involved with publishing the cables. Benkler argued the government had no case unless it could prove that somebody involved with WikiLeaks directly conspired with Manning.

What Benkler and many other constitutional scholars find insidious about the US government's approach to WikiLeaks is that since the government has no genuine case against the publishers, its assertion of WikiLeaks' illegality—no matter how groundless—"leaves room for various extralegal avenues that can be denied as not under your control to do the suppression work." The Obama administration can deny having directly ordered Amazon, PayPal, EveryDNS, and other businesses to sever ties with WikiLeaks, thus avoiding claims

that it has done anything unconstitutional or illegal. But its assertions about WikiLeaks nonetheless succeeded in making it more difficult for a politically controversial organization to publish and raise funds in the United States.

We have a problem: the political discourse in the United States and in many other democracies now depends increasingly on privately owned and operated digital intermediaries. Whether unpopular, controversial, and contested speech has the right to exist on these platforms is left up to unelected corporate executives, who are under no legal obligation to justify their decisions. The response to WikiLeaks' release of classified cables is a troubling example of private companies' unaccountable power over citizens' political speech, and of how government can manipulate that power in informal and thus unaccountable ways. This opaque manipulation is done in ways most people are unaware of or in some cases may even support, because they believe it does not affect them as law-abiding citizens. They may continue to believe that until they or someone they care about find *themselves* to be politically marginalized or vulnerable, or find that their rights have been violated for whatever reason.

CHAPTER 6

Democratic Censorship

Until April 2007, Kathy Sierra wrote a popular blog called "Creating Passionate Users," about how to design software that makes people happy. She was a sought-after speaker at technology conferences. Then death threats and sexually abusive comments drove her to halt all public speaking and writing. In a blog post explaining her decision, she wrote:

> As I type this, I am supposed to be in San Diego, delivering a workshop at the ETech conference. But I'm not. I'm at home, with the doors locked, terrified. For the last four weeks, I've been getting death threat comments on this blog. But that's not what pushed me over the edge. What finally did it was some disturbing threats of violence and sex posted on two other blogs . . . blogs authored and/or owned by a group that includes prominent bloggers.

The threats included altered photos of Sierra with a noose around her neck and a muzzle over her mouth. Some commenters described in graphic sexual language how they would slit her throat and then violate her in horrific ways.

For some reason, anonymous members of a website called meankids.org—who apparently disliked her positive outlook and friendly tone—had decided to target Sierra. Her case is an example of how the Internet can empower malevolent cyber-mobs to victimize innocent people, a disproportionate percentage of them women. The question is:

What can or should government do about this problem? All democracies are struggling to find the right balance between protecting innocent people from bullies and criminals on the one hand and on the other, preserving civil liberties and free expression on the Internet. Unfortunately, many governments are grasping at solutions that put them into conflict with multinational companies as well as human rights groups.

INTENTIONS VERSUS CONSEQUENCES

The Offensive Internet, published in early 2011, offers a collection of essays by prominent American intellectuals who are concerned that the rise of the Internet—and citizens' dependence on it for public discourse—threatens democracy in a number of troubling ways. Unattributed speech, they argue, tends to be irresponsible and inflammatory, causing the public discourse to deteriorate into mudslinging nastiness instead of focusing on issues and facts. Citing cases such as Sierra's, several essays in the book argue that the Internet can make it more difficult for at least some women to participate in public discourse—and hence public life and politics—without being subjected to vicious verbal attacks and even threats. In the essay "Civil Rights in an Information Age," University of Maryland law professor Danielle Citron describes an Internet with two faces: "One propels us forward with exciting opportunities for women and minorities to work, network, and spread their ideas online. The other brings us back to a time when anonymous mobs prevented vulnerable people from participating in society as equals."

Cass Sunstein, writing in his capacity as a Harvard law professor although the book was published while he was serving under Obama as head of the White House Office of Information and Regulatory Affairs, describes how anonymous online speech enables false rumors about public officials and current events to spread like wildfire and become ingrained in the minds of large segments of a nation's or region's population. "The marketplace of ideas," Sunstein writes, "will not work well if social influences ensure that false rumors can spread and become entrenched." He calls for laws to deter people from spreading damaging

falsehoods. He concludes that "some kind of chilling effect on false statements of fact is important—not only to protect people against negligence, cruelty, and unjustified damage to their reputations—but also to ensure the proper functioning of democracy itself." Sunstein does not explain how this approach would work, who would have the authority to draw the line between "spreading damaging falsehoods" and publishing controversial analysis or opinions that government authorities believe to be false but that other people genuinely believe to be true, and where such a line would be drawn. Countries best known for punishing people for "spreading rumors" include China, Russia, and Ben Ali's Tunisia.

Sunstein and his coauthors describe problems that are genuinely troubling and that could well erode democracy by reinforcing tyrannies of the majority and driving reason and fact to the margins of the democratic discourse. But the only direct way to prevent inflammatory speech is to eliminate anonymity so that everybody can be held accountable for what they write or upload onto the Internet. As Sunstein must be well aware, American democracy owes its existence in part to anonymity: anonymous pamphlets and tracts like *The Federalist* played an important role in building broader public support not only for a revolution but for a completely untested, experimental, new form of government.

Constitutional lawyer Lee Bollinger, in a recent book advocating a global commitment to protecting free speech, put it this way: "Political majorities and government officials cannot be trusted to exercise the power of censorship in a moderate fashion. Intolerance is natural, especially in times of stress. Given the opportunity to censor, people will censor, particularly when they feel anxious or threatened." Can Sunstein and his coauthors be so naive as to think that power holders in the twenty-first-century United States are different from power holders in any other place or time?

The digital networks and platforms that citizens depend upon are designed, owned, operated, and governed by the private sector. Thus, when democratic governments try to respond to public demands to counter all the "bad" speech online, the job of controlling speech is often delegated to private intermediaries. Yet these private intermediaries are

under no obligation to uphold citizens' rights to free expression and assembly. Their interest in guarding anonymous users' identity from government discovery is generally weak, given that the operational costs of defying government orders often appear to outweigh the risks of upsetting some customers—certainly in the short to medium term. If government is empowered to control speech and corporations have little incentive to protect speech, two powerful actors can potentially thwart citizens' freedom of speech in the digital public sphere.

South Korea, one of the most wired nations on earth, with the world's highest high-speed Internet penetration, serves as a cautionary example. In 2005, a young woman was riding the subway with her dog when it defecated on the floor. A fellow passenger proceeded to capture the scene on video as people around her reacted with disgust and outrage when she refused to clean up her dog's mess. The video went viral on the Internet, and she became globally famous as the "dog poop girl." To harass her, cyber-vigilantes quickly discovered who she was and where she lived; she reportedly had to go into hiding, get plastic surgery, and change her identity. Cyber-harassment has already caused a number of celebrity suicides there, according to numerous reports in the national and international media. A national poll in 2006 revealed that 85 percent of South Korean high school students were under stress from cyber-bullying. Not surprisingly, many South Koreans felt that things had gotten out of control, and voters have clamored for their elected representatives to do something.

The result was a law stipulating that all websites with more than 100,000 visitors per day must require users, when creating accounts, to supply not only their real names and addresses but also their national ID card numbers—which happen to be connected to a very efficient national database. Anonymity, South Korean legislators had come to believe, was undermining social stability, enabling cyber-mobs to harass innocent people and cyber-vigilantes to ostracize and shame people for less-than-admirable but nonetheless not criminal behavior. But this legal solution pursued by a democratically elected parliament ended up being used by economically and politically powerful people in South Korea to stifle speech they happened to find threatening.

In early 2009, South Korean blogger Park Dae-sung, aka Minerva, was arrested and jailed for four months on charges of "spreading false information to harm the public interest." His popular and influential postings on one of South Korea's most popular Internet platforms, Daum, provided critical analysis of his country's economic policies and financial situation. Because his writings influenced readers' investment decisions, he was accused by many in the government and media of having undermined South Korea's financial markets in 2008. Park claimed that he merely wanted to write about truths that seemed obvious to him but that the mainstream media were too timid to report—given their close relationships with the regime of President Lee Myung-bak and their need to obtain broadcasting licenses. Herein lies the dangerous slippery slope in legislation to curb anonymity.

Despite the fact that Park published his popular postings under a pseudonym, government investigators were easily able to identify him because he had to register with his real name, address, and ID number. Park was eventually acquitted (the court determined that he believed what he was writing and thus had not intentionally spread rumors), but only after spending four months in jail.

Park's case is only one of many. In early 2010, for example, seventeen people were charged with "spreading false information" after challenging the government's account of how a North Korean submarine had sunk a South Korean warship. This law, plus the real-ID requirement for Internet companies, prompted Google to disable uploading or comments on its Korean YouTube service in 2009. Citing a concern for South Korean Internet users' right to freedom of expression, a statement on the company blog declared, "We believe that it is important for free expression that people have the right to remain anonymous, if they choose."

Though the South Korean Constitutional Court eventually ruled in December 2010 that the law against "spreading false rumors" was unconstitutional, the real-ID registration requirement remained in place until mid-2011. In July the people of South Korea learned a painful lesson about why excessive data retention and ID requirements can make citizens less rather than more secure. The personal information including

national ID numbers of some 35 million South Koreans (out of a total population of 50 million) was stolen from the servers of SK Communications, operator of the country's third-most popular Web portal. Security experts traced the attack back to computer servers in mainland China. By early August, the number of South Korean ID numbers available for sale on Chinese websites was reported to have skyrocketed. (Chinese gamers covet accounts on South Korean online gaming sites but cannot gain access without a South Korean ID number, which has created a lively market for South Korean identities.) In the wake of the attack, the government announced that it would gradually phase out the real-name verification policy.

The Indian government's approach to controlling hate speech and suspected terrorist activity online has also raised concerns about whether the costs could ultimately outweigh the benefits. A new law that went into effect in late 2009 holds domestic and international Internet companies—including Yahoo, Facebook, YouTube, and Twitter—accountable for helping to maintain "public order, decency, or morality." Companies are expected to take the initiative to remove potentially inflammatory material. Failure to comply can result in jail terms of up to seven years for executives. The main impetus behind the law is religious violence, an ancient but still current problem in India that can be inflamed by hate-filled postings on the Internet.

Because India's Internet penetration (be it high-speed broadband or low-speed dial-up) remains quite low—under 10 percent of the population—the 2009 law was not a high priority for most Indian human rights groups. But then in April 2011, the Ministry of Communications and Information Technology went several steps further. Under new rules, Internet companies would be expected to remove within thirty-six hours any content regulators designated as "grossly harmful," "harassing," or "ethnically objectionable." Indian free speech advocates have vowed to challenge the rules' constitutionality. As Pranesh Prakash of the Center for Internet and Society in Bangalore put it, "The Indian Constitution limits how much the government can regulate citizens' fundamental right to freedom of speech and expres-

sion. Any measure afoul of the constitution is invalid." Google publicly protested the rules in a statement warning that "if Internet platforms are held liable for third party content, it would lead to self-censorship and reduce the free flow of information."

The previous year, Google ran afoul of Italian law as well as public sentiment favoring stronger control of online speech to protect innocent children and the disabled from harassment. In early 2010 an Italian judge handed down criminal sentences to four top Google executives (including David Drummond, the senior vice president who around the same time was busy handling the aftermath of Google's "new approach" to China) because YouTube staff had not been quick enough to remove all copies of a video of an autistic child being bullied by his classmates. The core issue is a tough one for democracies in the Internet age: When awful people put ghastly video on the Internet, with devastating consequences to innocent people, without the consent of the people appearing in the video, who should be held responsible and punished? Google's lawyers argued that staffers acted in good faith and removed the offending video as soon as they were aware of it. The Italian prosecutors countered that Google nonetheless failed to do enough—quickly enough—to protect an innocent child.

Google is not alone; Internet companies around the world face mounting pressure from governments not just to block websites but to delete a wide range of content from the Internet completely, as well as to track what their users are doing so they can be prosecuted or cut off if they do anything illegal. One way to compel censorship and surveillance by companies is to hold them legally responsible for what their users do with their services. The legal term for this practice is "intermediary liability," because the *intermediaries*, or companies transmitting or hosting users' communications or other content, are held *liable* for their users' and customers' behavior. In countries such as China, this arrangement is precisely the legal mechanism that enables an unaccountable government to delegate the bulk of censorship and surveillance to the private sector. In countries with a free press, independent courts, and competitive democratic politics, the problem is less severe.

Even so, civil liberties groups have good reason to be concerned that when excessive liability is placed on intermediaries, companies end up taking on censorship and surveillance functions without sufficient transparency, accountability, or public oversight.

It is at this newly forged digital intersection between corporate and political power where battles over freedom and control are being waged throughout the democratic world. In a January 2011 report titled *The Slide from "Self Regulation" to Corporate Censorship*, the Brussels-based nonprofit European Digital Rights Initiative (EDRI) warned that even though European democracies have not set out to create a "privatized police state," they may inadvertently be heading in that direction, thanks to growing pressure by governments on companies to police themselves. It is increasingly the norm in Europe for Internet companies to have "investigative, monitoring, policing, judging and sanctioning powers delegated to them, occasionally through legislation but, far more frequently, by coercion or by weakening or redefining the protections that they have been able to avail of up until now." As a result, wrote EDRI director Joe McNamee, "intermediaries' own consumers are increasingly being treated as 'the enemy.' Their Internet access is being increasingly blocked, logged, spied upon, restricted and subjected to sanctions imposed by the intermediaries, who fear legal liability for the actions of their clients." The implications, McNamee warns, threaten the core of the democratic enterprise, thanks to "a general abandonment of the traditional concept of the rule of law and the role of the judiciary. The result is the 'death by a thousand cuts' of traditional policing and judicial transparency."

SAVING THE CHILDREN

One example of extrajudicial enforcement is the United Kingdom's Internet Watch Foundation (IWF), a private nonprofit group that collects complaints from the public about websites containing child pornography, then develops a list of banned sites. This list is used "voluntarily" by all of the UK's major Internet service providers, and most of the content on the IWF's blacklist is what most people would consider "legitimately

harmful to children." But sometimes the IWF's decisions are controversial: in the fall of 2008 the group's overzealousness made Wikipedia inaccessible for the better part of a day to a large number of British Internet users, because the publicly edited online encyclopedia entry about the rock band Oasis included an album cover depicting an unclothed prepubescent girl. Freedom House, a US-based human rights and democracy organization that tracks global free speech trends, points out that the IWF's "procedures and policies are not transparent. The blocking criteria lack clarity, and the internal appeal process is inadequate. There is no judicial or governmental oversight of the IWF's activities."

Many democracies now deploy national-level filtering systems through which all ISPs (or in some cases most major ones) are compelled to block designated lists of websites to address public concerns about child pornography and other illegal activities conducted on the Internet. The United States does not have a nationwide Internet filtering system, though many school districts, public libraries, and other public networks maintain their own blacklists. But according to the Open Net Initiative, the number of countries that censor the Internet nationwide has gone from merely a handful a decade ago to almost forty today. This includes the obvious suspects, such as China, Iran, Vietnam, Saudi Arabia, and Tunisia. But the censorship club's fastest-growing membership segment consists of democracies, including the United Kingdom, France, the Netherlands, Australia, South Korea, India, and Turkey. Ronald Deibert, director of the Citizen Lab at the University of Toronto, which coordinates much of the Open Net Initiative's censorship research, wrote in the 2008 book *Access Denied,* "In less than a decade, the Internet in Europe has evolved from a virtually unfettered environment to one in which filtering in most countries, particularly within the European Union, is the norm rather than the exception."

Finland, Sweden, Denmark, and the Netherlands were the first countries in Europe to begin filtering content at the national level. In March 2011, the French constitutional court upheld a controversial new law giving the Ministry of Interior the power to instruct ISPs to block websites containing child pornography, despite criticisms by free speech

groups about the lack of oversight in determining what websites are placed on the blacklist. Then in May 2011, the Law Enforcement Working Party of the Council of the European Union, the EU's central legislative and decision-making body, issued a proposal to create a "single European cyberspace" that would block "illicit content" at Europe's borders.

Concerned that politicians are grasping at ineffectual solutions to a genuine problem, in early 2011 Malcolm Hutty, president of the European Service Providers' Association, wrote a letter to the European Parliament calling for an end to Internet filtering, calling it an "inefficient measure." In debating the issue, some members of the European Parliament pointed out that a website campaigning *against* child pornography was blocked twice in the Netherlands. Complaints abound about "collateral filtering"—the accidental blocking of websites that are unrelated to the stated reason for setting up the filtering system.

Even more disturbing, a growing body of academic research shows that Internet filtering has done little to stop the actual exploitation of real children and may even be exacerbating the problem. In late 2009 a team of academic researchers from France, Germany, the Netherlands, and Ireland published a research paper titled "Internet Blocking: Balancing Cybercrime Responses in Democratic Societies." After examining the impact of censorship on child pornographers, they reached a disturbing conclusion: though Internet filtering makes criminals' websites invisible to the general public, people who are determined to access them can easily figure out how to do so. Furthermore, the censorship does nothing to stop or bring to justice the people who are exploiting children in the first place. Nor does this kind of censorship actually stop criminals from trafficking in children and distributing child porn via e-mail or file-sharing services.

In some countries, concerned citizens have successfully reversed or stopped the implementation of national censorship schemes. In Australia a proposed national censorship system officially aimed at child porn and terrorism met with strong opposition. In March 2009, when the idea was first being debated, WikiLeaks published a secret government list of 2,935 websites that Internet service providers would be required to block

as part of a test run. It turned out that the content went beyond child porn and terrorism to include online poker and euthanasia. For reasons nobody could explain, a few businesses with no ties to child porn or other crimes also turned up on the list—including the offices of a dentist in Queensland. The point was that even in democracies, secret censorship lists end up censoring things that go beyond the original mandate—whether by mistake or on purpose. Once websites get on the list, it is difficult for them to be removed, because the list itself is secret.

In 2009 the German Parliament passed an Internet censorship law aimed at protecting children. Free speech groups pointed out that the list of websites to be blocked from public view was maintained by the police without any mechanism for public oversight. Immediately after the law was passed, a number of German politicians suggested that the list be extended to Islamist websites, video game sites, and gambling sites, and book publishers have suggested it would also be nice to block file-sharing sites while they are at it. Once the censorship mechanism was set up, the question became: Could Germany's political and legal systems prevent this mechanism from being abused? Civil liberties groups argued that abuse was inevitable. They eventually won over enough members of Parliament, and the law was overturned in early 2011.

It is thus an undeniable fact that democratic societies face urgent problems—sometimes magnified or accelerated by the Internet—for which voters are demanding solutions from their leaders. Politicians tend to grasp at solutions like censorship and surveillance because they seem expedient and practical in the democratic context but nevertheless invite abuse. Yet solutions to these problems must not make it more difficult for dissent and protest by weaving censorship and surveillance deeply into the legal and technical fabric of the global Internet. It is imperative that voters, politicians, and companies of the world's democracies gain greater awareness of the need to find innovative ways of addressing problems that will not require citizens to pay for security with their freedom.